IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH OF: THE RESIDENCE LOCATED AT 163 JESSE BROWN ROAD BOONE, NORTH CAROLINA 28607	Case No. 3:22mj31 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Jacob R Guffey, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am investigating the activities of the social media account belonging to Jason Ian Kendrick (SUBJECT), who resides at 163 Jesse Brown Road, Boone, North Carolina (NC), 28607 (SUBJECT RESIDENCE). As will be shown below, there is probable cause to believe that SUBJECT used his social media account to transport, possess, and distribute child pornography, in violation of 18 U.S.C. §§ 2252A(a)(1), (a)(2) and (a)(5)(b). I submit this Application and Affidavit in support of a search warrant authorizing a search of the SUBJECT RESIDENCE as further described in Attachment A. Located within the premises to be searched, I seek to seize evidence, fruits, and instrumentalities of the forgoing criminal violations, which relate to the knowing transportation, receipt, possession, and distribution of child pornography. I request authority to search the entire premises, including the residential dwelling, vehicles, located on the property, or any outbuildings such as detached garage, sheds, or barns. In addition, I request authority to search any computer and computer media located therein where the items specified in Attachment B, may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crime.

2. I am a Special Agent of the United States Department of Justice, Federal Bureau of Investigation (FBI), and have been so employed since April 2008. I am currently assigned to

the Charlotte Division, Hickory Resident Agency. In this capacity, I am assigned to investigate cases involving child pornography, corporate fraud, public corruption, and similar violations. From 2012 to 2015, I worked on the Navajo Indian Reservation, in the Albuquerque Division, Gallup Resident Agency. At that assignment I conducted and participated in numerous death investigations, child sexual assaults, and other federal crimes occurring with the boundaries of Indian Country. From 2008 to 2012 I investigated Health Care Fraud in the Miami Division. I have personally been the case agent for numerous investigations that have resulted in the indictment and conviction of numerous subjects. I have also participated in the ordinary methods of investigation, including but not limited to, consensual monitory, physical surveillance, interviews of witnesses and subjects, and the use of confidential informants. I have executed numerous search warrants and seized evidence. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

3. I am an investigative or law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7), and am empowered by 18 U.S.C § 3052 to conduct investigations of, and to make arrests for, violations of federal criminal statutes.

4. The facts set forth in this Affidavit come from my personal observations, my training and experience, evidence gathered pursuant to subpoenas, government records requests, and information obtained from other agents and witnesses. Because this Affidavit is submitted for the limited purpose of establishing probable cause to support the contemporaneously filed Applications, it does not include each and every fact known to me or to other investigators.

5. Based on my training and experience and the facts as set forth in this Affidavit, there is probable cause to believe that evidence, fruits, and instrumentalities of the violation of

Title 18 U.S.C. § 2252A, transportation, access with intent to view, possession, receipt, and distribution of child pornography are presently located at SUBJECT RESIDENCE.

STATUTORY AUTHORITY

6. This investigation concerns alleged violations of Title 18, U.S.C. § 2252A(a)(1), (a)(2) and (5)(B), relating to material involving the sexual exploitation of minors.

a. Title 18, U.S.C. § 2252A(a)(1) makes it a crime to knowingly mail, or transport, or ship, using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means including by computer, any child pornography.

b. 18 U.S.C. § 2252A(a)(2) makes it a crime to knowingly receive or distribute (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

c. Title 18, U.S.C. § 2252A(5)(B) prohibits knowingly possessing or knowingly accessing with intent to view any book, magazine, periodical, film, video tape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

7. The following definitions apply to this Affidavit and Attachment B:

a. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child Pornography" includes any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

c. "Computer" refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." *See* 18 U.S.C. § 1030(e)(1).

d. "Computer hardware" consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes

any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

e. "Computer passwords and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

f. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

g. "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. Like a phone number, no two computers or network of computers connected to the internet are assigned the same IP address at exactly the same date and time. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

i. "Minor" means any person under the age of 18 years. *See* 18 U.S.C. § 2256(1).

j. "Sexually explicit conduct" refers to actual or simulated (a) sexual intercourse (including genital-genital, oral-genital, or oral-anal), whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals or pubic areas of any person. *See* 18 U.S.C. § 2256(2)(A).

k. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

l. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including, but not limited to, phonograph records, printing, typing); or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

8. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology, and the Internet have revolutionized the manner in which child pornography is produced and distributed.

9. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

10. Child pornographers can transpose photographic images from a camera into a computer-readable format with a scanner. With digital cameras, the images can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

11. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

12. The Internet affords collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

13. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

14. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

15. Based on my knowledge, training, and experience, I know that computer storage devices, such as a computer hard drive, can store information for long periods of time. Even when a user deletes information from a device, it can sometimes be recovered with forensics tools. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

16. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

17. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto optical, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

18. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, deleted, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

19. To fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware

drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

20. Furthermore, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

21. It is my experience with similar cases that individuals who download, produce, and or distribute child pornography, often collect those files. The individuals who collect and produce child pornography store it on their electronic devices so that they may view it later. They also collect it so they may have something to use as barter for additional child pornography on the internet.

22. *Forensic evidence.* As further described in Attachment B, this Application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the

storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that

log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

23. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete

electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

24. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection to determine whether it is evidence described by the warrant.

INFORMATION REGARDING KIK MESSENGER

25. Kik Messenger (hereinafter, "Kik") is a free instant messaging mobile application designed and previously owned by Kik Interactive Incorporated, a company based in Waterloo, Canada[1]. Kik uses the Internet to allow users to send and receive instant messages, photos and videos. During the account registration process, users are prompted to create a username, which cannot later be changed, and a display or vanity name, which other users initially see when communicating. During the registration process, users are also asked to provide an email address, date of birth, user location and a profile picture. Email addresses can be "confirmed," which means the user verified the email address is valid by clicking a link sent from Kik to the provided email address, or "unconfirmed," which means the email address is invalid, or the user

[1] Kik was purchased in or about October 2019 by MediaLab, Inc., a U.S.-based technology company headquartered in California.

did not click on the link from Kik. One key feature of Kik is that users are not required to provide accurate information during the account registration process.

26. Once an account is created, a user is able to locate other users through a search feature. The search feature generally requires a user to know an intended recipient's username to locate them. Once connected, Kik users can share messages, images, and videos. Kik also allows users to create chatrooms, through which groups of up to 50 users can exchange messages and digital files. These chatrooms, commonly referred to as "Kik Groups," are administered by the user who created the chatroom, and this user has the authority to add, remove, and ban other users from the group, as well as to promote other users to "administrator." This is true for both private and public chatrooms. Many public groups are created with a group code that contains a "hashtag" (e.g., "#KikTeens"), allowing the group or chatroom to be located more easily.[2] Specifically, a user will search for a public group using a term or word associated with the group name, which is often contained in the hashtag. Once a group is created, Kik users can engage in a "group chat" and exchange messages and content.

27. According to Kik's Terms of Service, which each user must acknowledge when creating an account, it is a violation of the agreement to use Kik to upload, post, comment on, or store content that is obscene, offensive, contains pornography, or is harmful to minors in any way. These Terms of Service specifically state that "…[Kik] may review, screen and delete your User Content at any time if we think it may violate these Terms. You are responsible for the User Content that you send through the Services, including for back up of such content."

28. Based on my training and experience in child exploitation investigations, I am aware that Kik is a prominent meeting place for individuals seeking to share child pornography

[2] The hashtag locating feature is not typically available for private groups.

and engage in child exploitative dialogue. I have investigated several offenders who used Kik to transport, distribute, and receive child pornography. Based on information obtained from interviews with some of these offenders, I am aware that Kik is a preferred platform for child exploitation offenders because the application facilitates anonymous communication, which assists offenders in avoiding detection by law enforcement.

FACTS IN SUPPORT OF PROBABLE CAUSE

29. On or about January 26, 2021, an undercover FBI agent with the Atlanta FBI Field Office was conducting surveillance on the messaging application Kik and identified user, "jik2kool," (SUBJECT ACCOUNT) as being a member of a Kik chat group, herein referred to as "Group 1". Additionally, the agent observed Kik SUBJECT ACCOUNT share child pornography within "Group 1". The name listed with the Kik profile was, "J T". During a review of the undercover session, your Affiant observed the following activity by SUBJECT ACCOUNT:

a. On or about January 26, 2021, SUBJECT ACCOUNT asked the group, "Trade?" To which a user replied, "Whacha got?" SUBJECT ACCOUNT then shared video "IMG_1824.mp4" of a female under the age of 16, who was nude from the waist up. The female in the video says, "Please daddy, I want you to cum on my face. She then puts a pacifier into her mouth. The other user replied to SUBJECT ACCOUNT, "Sorry dude, a little old for my taste."

b. SUBJECT ACCOUNT then shared video "IMG_1825", which depicted a nude female under the age of 10. An adult male ejaculates on her. The male asked the female to, "say it over and over again". To which she replies, "cum for me daddy". SUBJECT ACCOUNT then writes, "Better".

c. SUBJECT ACCOUNT shared a video of a female who appeared to be under the age of 18 who is masturbating.

d. SUBJECT ACCOUNT, shared two images of females whose ages appeared to be over the age of 18.

30. On or about February 19, 2021, the FBI Atlanta Field Office received the following information from Kik via MediaLab, Inc through an administrative subpoena, regarding, SUBJECT ACCOUNT:

e. Email: jik2kool@gmail.com (unconfirmed)

f. Registration: August 3, 2020 08:54:32

g. Birthday: February 2, 1985

h. Phone model: iPhone

i. Most recent IP Address: 47.135.146.234 on February 18, 2021 17:02:35 UTC

31. On or about February 22, 2021, FBI Atlanta Field Office submitted an administrative subpoena to Charter Communications to obtain the subscriber information regarding IP address 47.135.146.234 on February 18, 2021, at 17:02:35 UTC.

32. On or about March 6, 2021, FBI Atlanta Field Office received subscriber information from Charter Communications through an administrative subpoena regarding IP Address, 47.135.146.234. The following information was provided by Charter Communications:

j. Subscriber: Terra Olive Kendrick

k. Address: 163 Jesse Brown Road, Boone, NC, 28607-8852 (SUBJECT RESIDENCE)

l. Username: terraolivekendrick@charter.net

m. Phone (828)964-6008

33. Although SUBJECT ACCOUNT accessed the Kik account from various IP Addresses, a review of the records from Kik showed that SUBJECT ACCOUNT accessed the Kik account from IP Address 47.135.146.234 (SUBJECT IP ADDRESS) throughout the duration of the subpoena return, spanning from January 21, 2021 through February 18, 2021.

34. On or about March 12, 2021, Agents from the FBI Atlanta Field Office conducted an Internet search for Terra Kendrick, Boone, NC. One of the results was for Terra Olive and included the reference to SUBJECT. The Agent observed KENDRICK's initials matched the "jik" portion of the Kik username, "jik2kool".

35. On March 12, 2021, the Agent from the FBI Atlanta Field Office conducted a law enforcement database check for both Terra Olive Kendrick and SUBJECT and found they both had the address SUBJECT RESIDENCE.

36. On or about June 7, 2021 and December 17, 2021, your Affiant conducted a driver's license check for SUBJECT and found his listed address was SUBJECT RESIDENCE.

37. On or about July 21, 2021 and December 17, 2021, your Affiant reviewed Watauga County land records and found that SUBJECT and Terra M Olive were listed as the owners of SUBJECT RESIDENCE.

38. On or about June 14, 2021, your Affiant served MediaLab, Inc., with a preservation letter for the records related to SUBJECT ACCOUNT.

39. On July 23, 2021, your Affiant conducted physical surveillance at SUBJECT RESIDENCE and observed a vehicle parked on the property whose license plate resolved to SUBJECT.

40. On or about August 30, 2021, your Affiant obtained a search warrant signed by the Honorable David C. Keesler United States Magistrate Judge, Western District of North

Carolina (3:21mj204). The search warrant was served to Media Lab on or about September 2, 2021, and compelled Media Lab to produce records pertaining to SUBJECT ACCOUNT. Due to some difficulties with your Affiant's email account, you Affiant did not observe the receipt of the records from Media Lab until on or about November 15, 2021.

41. On or about December 15, 2021 your Affiant was able to review the search warrant production after procuring and obtaining software which was able to process the data produced by Media Lab. Media Lab produced activity between SUBJECT ACCOUNT and other Kik users. Of use to this investigation, Media Lab provided dates and times, SUBJECT ACCOUNT's IP Address for each transaction, videos, and images sent by SUBJECT ACCOUNT. Media Lab did not provide text conversations.

42. The following is a summary of some of the activity view by your Affiant:

a. On or about May 19, 2021, SUBJECT ACCOUNT sent a Kik user an image of a female who appeared to be under the age of 12, who had an adult penis in her hand. The image was sent from SUBJECT IP ADDRESS. The image was then also sent to an additional Kik user.

b. On or about June 7, 2021, SUBJECT ACCOUNT sent a Kik user a video which was approximately 41 seconds long. The video was of a female who appeared to be under the age of 18 who had a nude female's vagina on her mouth. The video was sent from SUBJECT IP ADDRESS. The video was also sent to 4 additional Kik users.

c. On or about June 7, 2021, SUBJECT ACCOUNT sent a Kik user a video which was approximately 48 seconds long. The video was of a female who appeared to be under the age of 12 who had her hand on the vagina of a female who was nude

from the waist up. The second female appeared to be under the age of 16 and was wearing underwear. They were laying on a bed with their mouths touching. The video was sent from SUBJECT IP ADDRESS. The video was also sent to an additional Kik user.

d. On or about June 14, 2021, SUBJECT ACCOUNT sent a Kik user a video which was approximately 13 seconds long. The video was of an adult female with her tongue on the vagina of a female who was nude from the waist down and who appeared to be under the age of 12. The video was sent from SUBJECT IP ADDRESS. The video was also sent to 1 additional Kik user.

e. On or about June 14, 2021, SUBJECT ACCOUNT sent a Kik user a video which was approximately 1 minute and 11 seconds long. The video was of a nude female who appeared to be under the age of 12, who had an adult penis in her hand.

43. On or about June 7, 2021, SUBJECT ACCOUNT sent a Kik user an image which resembled SUBJECT. The image was sent from SUBJECT IP ADDRESS. Several other images and videos resembling SUBJECT were sent to various Kik users from SUBJECT ACCOUNT and SUBJECT IP ADDRESS.

44. On January 11, 2022, your Affiant served Charter Communications with an Administrative Subpoena requesting the subscriber information for SUBJECT IP ADDRESS during the dates and times for the activities referenced in paragraph 42 of this Affidavit. Your Affiant also requested the dates of service for the subscriber's account.

45. On January 17, 2022, Charter Communications provided the following response:

a. For the dates and times provided by your Affiant the IP Address belonged to account holder Terra Olive Kendrick, who your Affiant understands to be SUBJECT's wife.

b. For those same dates and times, the IP Address belonged to service address: SUBJECT ADDRESS.

c. The lease date for the MAC Address for the Charter Communications device used in the home to connect to the Internet had a start date of August 1, 2020 and an end date of January 12, 2022. In your Affiant's experience Charter Communications lists the end date of the lease as the date and time they check the status of the device/account when responding to a legal request. Your Affiant understands that the end date does not exclusively mean that the account is no longer active.

CONCLUSION

46. Based on the aforementioned information, your Affiant respectfully submits that there is probable cause to believe that SUBJECT acted through SUBJECT ACCOUNT to transport, posses, and distribute child pornography. Your Affiant respectfully submits that there is probable cause to believe that SUBJECT has violated 18 U.S.C. §§ 2252A. Additionally, there is probable cause to believe that evidence of criminal offenses, namely, violations of 18 U.S.C. §§ 2252A(a)(1), (a)(2) and (a)(5)(B), is located in the SUBJECT RESIDENCE described in Attachment A, and this evidence, listed in Attachment B to this Affidavit, which is incorporated herein by reference, is contraband, the fruits of crime, or things otherwise

criminally possessed, or property which is or has been used as the means of committing the foregoing offenses.

Respectfully submitted,

/s/ Jacob R. Guffey

Special Agent Jacob R Guffey
United States Department of Justice
Federal Bureau of Investigation

This affidavit was reviewed by AUSA Cortney Randall.

In accordance with Rule 4.1(b)(2)(A), the Affiant attested under oath to the contents of this Affidavit, which was submitted to me by reliable electronic means, on this 24th day of January, 2022, at 3:16 PM.

Signed: January 24, 2022

David C. Keesler
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

The residence, outbuildings, structures, appurtenances, and vehicles located at 163 Jesse Brown Road, Boone, North Carolina, 28607. The residence is described as a single-story home with red brick and a basement. There are 2 smaller buildings next to the residence.

ATTACHMENT B

Particular Things to be Seized

1. Instrumentalities of the violations contained within the Application for the search warrant at 163 JESSE BROWN ROAD, BOONE, NORTH CAROLINA, 28607:

a. any computer, computer system, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, hard drive and other computer related operation equipment, photographs and other visual depictions of such graphic interchange formats (JPG, GIF, TIF, AVI, and MPEG), electronic data storage devices (hardware, software, diskettes, backup tapes, CDs, DVD, flash memory devices, thumb drives, and other storage media); and any input/output peripheral devices, passwords, data security devices, and related security documentation;

b. books and magazines containing visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2)(A);

c. originals, copies, and negatives of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2)(A); and

d. motion pictures, films, videos, and other recordings of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2)(A).

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, “COMPUTER”):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. records of or information about Internet Protocol addresses used by the COMPUTER;

j. records of or information about the COMPUTER's Internet activity: firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

k. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet;

4. Any child pornography as defined by 18 U.S.C. § 2256(8);

5. Any and all records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of computer equipment found in the residence;

6. Documents and records regarding the ownership and/or possession of the searched premises;

7. Credit card information, bills, and payment records;

8. Information or correspondence pertaining to affiliation with any child exploitation websites;

9. Any material that is "child erotica";

10. Any correspondence/records indicating the true identity of any member or user of "Kik" and;

11. Any correspondence, e-mails, electronic messages, and records pertaining to "Kik"

As used above, the terms "records" and "information" refer to all forms of creation or storage, any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as prints, videotapes, motion pictures, or photocopies).

The term "computer" refers to all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions: desktop computers, notebook computers, mobile phones, tablets, server computers, smart phones, and network hardware.

The term "storage medium" refers to any physical object upon which computer data can be recorded. Examples are hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein.

If the government identifies seized materials, that are potentially attorney-client privileged or subject to the work product doctrine ("protected materials"), the Prosecution Team will discontinue review until a Filter Team of government attorneys and agents is established. The Filter Team will have no future involvement in the investigation of this matter. The Filter Team will review seized communications and segregate potentially protected materials, i.e. communications that are to/from an attorney, or that otherwise reference or reflect attorney advice. At no time will the Filter Team advise the Prosecution Team of the substance of any of

the potentially protected materials. The Filter Team then will provide all communications that are not potentially protected materials to the Prosecution Team and the Prosecution Team may resume its review. If the Filter Team concludes that any of the potentially protected materials are not protected (*e.g.*, the communication includes a third party or the crime-fraud exception applies), the Filter Team must obtain either agreement from defense counsel/counsel for the privilege holder or a court order before providing these potentially protected materials to the Prosecution Team.